(19) KOREAN INTELLECTUAL PROPERTY OFFICE

KOREAN PATENT ABSTRACTS

(11)Publication number: 1020040036228 A
(43)Date of publication of application: 30.04.2004

(21)Application number: 1020020065176
(22)Date of filing: 24.10.2002

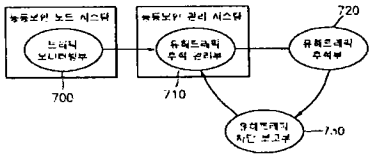
(51)Int. Cl H04L 12/22

(71)Applicant: ELECTRONICS AND TELECOMMUNICATIONS RESEARCH INSTITUTE

(72)Inventor: BANG, HYO CHAN
NA, JUNG CHAN
SON, SEUNG WON

(54) SYSTEM AND METHOD FOR DETECTING AND COPING WITH HARMFUL TRAFFIC IN NETWORK

(57) Abstract:



PURPOSE: A system and a method for detecting and coping with harmful traffic in a network are provided to protect a system and a network resource by detecting a harmful traffic, tracing a source of the harmful traffic and cutting off the source. CONSTITUTION: A traffic monitoring unit (700) periodically monitors change of traffic flowing into active security node systems and if there is a traffic change exceeding a pre-set reference value, the traffic monitoring unit(700) transmits event information to active security management systems. A harmful traffic tracing management unit(710) determines whether to trace the harmful traffic on the basis of the event information, generates a harmful traffic tracing unit(720) and transmits it to the active security node system. A harmful traffic tracking unit(720) detects an IP address having the traffic component exceeding the reference value, analyzes traffic transmitted from a corresponding source IP address by sessions, detects and cuts off session traffic exceeding the reference value, and transfers a corresponding result to the active security management system. A harmful traffic cut-off report unit(730) informs the active security management system of the result.

SYSTEM AND METHOD FOR DETECTING AND COPING WITH HARMFUL TRAFFIC IN NETWORK

Publication number:	KR20040036228
Publication date:	2004-04-30
Inventor:	BANG HYO CHAN; NA JUNG CHAN; SON SEUNG WON
Applicant:	KOREA ELECTRONICS TELECOMM
Classification:	
- international:	***H04L12/22;*** **H04L12/22;** (IPC1-7): H04L12/22
- European:	
Application number:	KR20020065176 20021024
Priority number(s):	KR20020065176 20021024

Report a data error here

Abstract of **KR20040036228**

PURPOSE: A system and a method for detecting and coping with harmful traffic in a network are provided to protect a system and a network resource by detecting a harmful traffic, tracing a source of the harmful traffic and cutting off the source. CONSTITUTION: A traffic monitoring unit(700) periodically monitors change of traffic flowing into active security node systems and if there is a traffic change exceeding a pre-set reference value, the traffic monitoring unit(700) transmits event information to active security management systems. A harmful traffic tracing management unit(710) determines whether to trace the harmful traffic on the basis of the event information, generates a harmful traffic tracing unit(720) and transmits it to the active security node system. A harmful traffic tracking unit(720) detects an IP address having the traffic component exceeding the reference value, analyzes traffic transmitted from a corresponding source IP address by sessions, detects and cuts off session traffic exceeding the reference value, and transfers a corresponding result to the active security management system. A harmful traffic cut-off report unit(730) informs the active security management system of the result.

10-2004-0036228

(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(51) Int. Cl.
H04L 12/22

(11) 공개번호 10-2004-0036228
(43) 공개일자 2004년04월30일

(21) 출원번호 10-2002-0065176
(22) 출원일자 2002년10월24일

(71) 출원인 한국전자통신연구원
대전 유성구 가정동 161번지
(72) 발명자 방효찬
대전광역시유성구신성동한울아파트111동1101호
나중찬
대전광역시유성구어은동한빛아파트121동206호
손승원
대전광역시유성구전민동엑스포아파트208동902호
(74) 대리인 이영필, 이해영

심사청구 : 있음

(54) 네트워크에서의 유해 트래픽 탐지 및 대응 시스템 및 방법

요약

본 발명은 네트워크의 유해트래픽 탐지 및 대응 시스템 및 방법에 관한 것으로서, 그 시스템은 능동 네트워크 보안 프레임 워크에서, 보안노드시스템으로 유입되는 트래픽의 변동을 감시하여 변동이 감지되면 보안관리 시스템으로 송신하는 트래픽모니터링부; 이로부터 유해트래픽 추적 여부를 결정하고, 보안노드시스템으로 전송하는 유해트래픽추적관리부; 및 기준치 초과 트래픽 성분을 갖는 IP 주소를 검출하고 IP 주소가 위치하는 보안노드시스템 상에서 IP 주소에서 송신되는 기준치 초과 트래픽을 검출 및 차단하고 그 결과를 보안관리 시스템으로 전달하는 유해트래픽추적부를 포함함을 특징으로 한다. 본 발명에 의하면, 대역폭 소모형 분산 서비스 거부 공격과 같은 유해 트래픽을 조기에 탐지하고, 그 근원지를 추적하여 원천봉쇄하는 할 수 있다.

대표도

도8

명세서

도면의 간단한 설명

도 1은 능동보안관리 프레임워크 및 메카니즘을 도시한 것이다.

도 2는 능동보안 시스템 플랫폼(Platform) 구조를 도시한 것이다.

도 3은 이동보안센서 처리 엔진 및 능동보안관리 엔진의 기능 블록을 도시한 것이다.

도 4는 능동보안관리 센서의 기능구조를 도시한 것이다.

도 5는 액티브 네트워크를 이용한 능동보안관리 프레임워크에서의 위장된(Spoofed) IP 역 추적 메커니즘 및 기능절차를 도시한 것이다.

도 6은 본 발명에 따른 유해 트래픽 탐지/대응 시스템이 기능하기 위한 액티브 네트워크를 이용한 네트워크 보안 프레임워크와 망 구성을 도시한 것이다.

도 7은 본 발명에 따른 유해 트래픽 탐지 및 대응 시스템을 블록도로 도시한 것이다.

도 8은 본 발명에 따른 유해트래픽 탐지 및 대응 시스템의 동작을 설명하기 위한 절차를 도시한 것이다.

발명의 상세한 설명

발명의 목적

발명이 속하는 기술분야 및 그 분야의 종래기술

본 발명은 네트워크 보안에 관한 것으로서, 더욱 상세하게는 액티브 네트워크를 이용한 보안 프레임 워크

상에서 네트워크의 트래픽 혼잡을 유발시키는 유해 트래픽을 탐지하고 대응하는 네트워크의 유해트래픽 탐지 및 대응 시스템 및 방법에 관한 것이다.

최근 들어 인터넷을 통한 사이버 공격의 형태가 다양해지고 복잡해지면서 단일 보안 시스템만으로는 이에 대한 효과적인 탐지 및 대응이 어려워지고 있다. 따라서 단일 보안 시스템들을 유기적으로 연관시키고 자동적으로 통합관리하기 위한 통합보안 관리 기술 및 통합 관제 시스템들이 제안되고 있다. 그러나 제한된 단일보안 관리 영역만을 중앙 집중적으로 관리하는 수동적인 보안 관리 체계로는 인터넷이라는 전 세계적인 광역 망을 통해 가해지는 사이버 공격을 막기에는 어려움이 있다.

더구나 분산서비스거부(Distributed Denied Of Service: 이하 'DDoS'라 한다) 공격은 매우 심각한 네트워크 보안 문제로 인식되고 있다. DDoS 공격은 정상적인 트래픽과 구별하기가 힘들어 사전에 예측하기가 곤란하며, 피해 규모가 네트워크 전역에 걸쳐 매우 크다. 또한 DDoS 공격의 대부분이 다량의 유해 트래픽을 네트워크에 유입시켜 망 전체의 자원을 고갈시키는 대역폭 소모형 공격 추세로 발전되고 있어 네트워크 보안 측면 뿐 만이 아니라 기존의 네트워크 자원 관리 측면에서도 매우 심각한 문제를 유발시키고 있다. 특히 이러한 DDos 공격은 피공격자 도메인(Domain)에서 해당 유해 패킷을 차단하더라도 전달 망에는 그대로 유해 트래픽이 유입되기 때문에 망 전체의 혼잡 및 자원 고갈은 해결되지 않는다. 따라서 기존의 국지적인 보안 구조로는 해결 할 수 없는 심각한 문제점들이 도출되고 있다. 이러한 상황으로 비추어 볼 때, 현실적으로 모든 DDoS 공격을 완전히 예측하고 대응할 수 있는 방안은 없지만, DDoS 공격으로 인한 네트워크 자원 및 서비스의 손실을 최소화 할 수 있는 탐지/대응 기술이 필요하다.

이를 위해서는 유해 트래픽을 사전에 감지해 내고, 유해 트래픽을 전송하는 해커 도메인 또는 보안관리 영역의 최초 유입점에서 유해 트래픽을 차단할 수 있는 능동적이고 지능적인 대응 기술이 필요하다. 이러한 기능을 실현하기 위해서는 수동적이고 정적인 기존의 통합 관리 방식 보다 유연하고 동적이며 분산적이고 협업적인 능동 보안 관리 메카니즘이 필요하다.

발명이 이루고자 하는 기술적 과제

본 발명이 이루고자 하는 기술적 과제는 액티브 네트워크를 이용한 보안 프레임 워크 상에서 분산 서비스 거부공격과 같이 네트워크의 트래픽 혼잡을 유발시키는 유해 트래픽을 탐지하여 대응할 수 있게 하는, 네트워크에서의 유해트래픽 탐지/대응 시스템을 제공하는 데 있다. 즉 본 발명은 액티브 네트워크를 이용한 네트워크 보안 프레임워크 상에서 네트워크의 트래픽 혼잡을 유발시키는 유해 패킷을 실시간으로 탐지하고 추적하여 유해 패킷이 유입되는 최초 접속점에서 해당하는 유해 트래픽을 차단함을 목적으로 한다.

본 발명이 이루고자 하는 다른 기술적 과제는 액티브 네트워크를 이용한 보안 프레임 워크 상에서 분산 서비스 거부공격과 같이 네트워크의 트래픽 혼잡을 유발시키는 유해 트래픽을 탐지하여 대응할 수 있게 하는, 네트워크에서의 유해트래픽 탐지/대응 방법을 제공하는 데 있다.

발명의 구성 및 작용

상기 기술적 과제를 달성하기 위하여 본 발명에 따른 네트워크에서의 유해트래픽 탐지/대응 시스템은, 분산된 적어도 둘 이상의 보안관리 영역을 포함하는 능동 네트워크 보안 프레임 워크에 있어서, 상기 보안관리 영역은 광역 망의 접속점에 위치하여 보안기능을 수행하는 보안노드 시스템 및 보안관리 영역에서 발생한 보안위배 행위에 대해 대응하고 보안상태를 제어하는 보안관리 시스템을 포함할 때, 상기 보안노드 시스템으로 유입되는 트래픽의 변동을 감시하고, 소정의 기준치를 초과하는 트래픽 변동이 감지되면 이에 대한 이벤트 정보를 당해 보안관리 영역의 보안관리 시스템으로 송신하는 트래픽모니터링부; 상기 보안관리 시스템으로 전달된 이벤트 정보로부터 유해 트래픽 추적 여부를 결정하고, 이를 당해 보안노드 시스템으로 전송하는 유해트래픽추적관리부; 및 소정의 기준치를 초과하는 트래픽 성분을 갖는 근원지 IP 주소와 목적지 IP 주소를 검출하고, 근원지 IP 주소가 위치하는 보안관리 영역에 위치하는 보안노드 시스템 상에서, 상기 근원지 IP 주소에서 송신되는 트래픽을 분석한 후 소정의 기준치를 초과하는 트래픽을 검출하여 차단하고 유해 트래픽 탐지 및 대응 결과를 해당 보안 관리 영역 내의 보안관리 시스템으로 전달하는 유해트래픽추적부를 포함함을 특징으로 한다. 또한 상기 네트워크에서의 유해트래픽 탐지 및 대응 시스템은 유해 트래픽 탐지 및 대응 결과를 최초에 유해 트래픽 추적을 요구한 능동보안관리 시스템에게 통보하는 유해 트래픽 차단 보고부를 더 구비함이 바람직하다.

상기 다른 기술적 과제를 달성하기 위하여 본 발명에 따른 네트워크에서의 유해트래픽 탐지 및 대응 방법은, 네트워크의 트래픽의 변동을 감시하여 소정이 기준치를 초과하는 트래픽 변동이 감지되면 이에 대한 이벤트정보를 송신하는 제1단계; 상기 이벤트정보를 수신하여 유해 트래픽 추적 여부를 결정하는 제2단계; 및 추적이 필요하다고 판단되면, 상기 소정의 기준치를 초과하는 트래픽의 근원지 주소를 검출하고, 상기 근원지 주소에서 송신되는 트래픽을 분석한 후 소정의 기준치를 초과하는 트래픽을 차단하는 제3단계를 포함함을 특징으로 한다.

상기 제2단계는 소정의 기준치를 초과하는 트래픽의 근원지 IP 주소 및 목적지 IP 주소를 검출하고, 상기 근원지 IP주소가 위치하는 네트워크 상의 소정의 시스템에서 상기 근원지 IP 주소로부터 송신되는 트래픽을 서비스 포트 별로 분석한 후 소정의 기준치를 초과하는 트래픽을 차단하는 단계임이 바람직하다.

상기 네트워크에서의 유해트래픽 탐지 및 대응 방법은 상기 제3단계의 유해 트래픽 탐지 및 대응 결과를 유해 트래픽 추적을 요구한 시스템에 통보하는 단계를 더 구비함이 바람직하다.

상기 다른 기술적 과제를 달성하기 위하여 본 발명에 따른 네트워크에서의 유해트래픽 탐지 및 대응 방법은, 분산된 적어도 둘 이상의 보안관리 영역을 포함하는 능동 네트워크 보안 프레임 워크에 있어서, 상기 보안관리 영역은 광역망의 접속점에 위치하여 보안기능을 수행하는 보안노드 시스템 및 보안관리 영역에서 발생한 보안위배 행위에 대해 대응하고 보안상태를 제어하는 보안관리 시스템을 포함할 때, 상기 보안노드 시스템으로 유입되는 트래픽의 변동을 감시하고, 소정의 기준치를 초과하는 트래픽 변동이 감지되면 이에 대한 이벤트 정보를 상기 보안관리 시스템으로 송신하는 제1단계; 보안관리 시스템으로 전달된 이벤트 정보로부터 유해 트래픽 추적 여부를 결정하고, 유해 트래픽 추적 센서를 생성하여 관리 도메인에 위치하는

보안노드 시스템으로 전송하는 제2단계; 및 소정의 기준치를 초과하는 트래픽 성분을 갖는 근원지 IP 주소와 목적지 IP 주소를 검출하고, 근원지 IP 주소가 위치하는 로컬 네트워크 상의 보안노드 시스템들에게 자신을 복제하여 전송하며, 해당 능동보안노드 시스템으로 이주한 후에는 해당 근원지 IP 주소에서 송신되는 트래픽을 서비스 포트 별로 분석한 후 소정의 기준치를 초과하는 트래픽을 검출하여 차단하는 제3단계를 포함함을 특징으로 한다.

상기 제2단계는 보안관리 시스템으로 전달된 이벤트 정보로부터 유해 트래픽 추적 여부를 결정하고, 유해 트래픽 추적 센서를 생성하여 관리 도메인에 위치하는 보안노드 시스템으로 전송하고 유해 트래픽 탐지 및 대응 결과를 해당 보안 관리 영역 내의 보안관리시스템으로 전달하는 단계이고, 유해 트래픽 탐지 및 대응 결과를 최초에 유해 트래픽 추적을 요구한 보안관리 시스템에게 전달하는 단계를 더 구비함이 바람직하다. 그리고 상기 이벤트 정보는 트래픽 감사 센서를 통해 보안관리 시스템으로 송신함이 바람직하다.

그리고 상기 기재된 발명을 컴퓨터에서 실행시키기 위한 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록매체를 제공한다.

이하, 첨부된 도면을 참조하여 본 발명의 바람직한 실시예를 들어 상세히 설명한다. 본 발명의 바람직한 실시예는 액티브 네트워크를 이용한 네트워크 보안 프레임 워크 상에서 동작된다. 따라서 액티브 네트워크를 이용한 네트워크 보안 프레임 워크에 대한 설명을 먼저 하기로 한다.

상술한 종래 기술의 문제점을 극복하기 위해 향후의 보안 기반 구조는 분산된 다수의 보안관리 영역간에 상호 협력적이고 결합적인 보안관리가 가능해야 하며, 새로운 보안 메커니즘 및 프로토콜을 쉽게 수용할 수 있는 유연하고 개방적인 보안 메커니즘을 제공할 수 있어야 한다. 이러한 보안환경의 변화에 따르는 요구사항을 반영할 수 있는 보안 기반 구조로서 액티브 네트워크를 이용한 능동보안 관리 프레임워크가 요청되고 있다. 즉 향후의 네트워크 보안 기반 구조는 단일 네트워크 내에서의 방어적인 보안 기능을 제공하는 현재의 보안 기반 구조를 광역 망에서 기능할 수 있도록 확장하고 새로운 보안 메커니즘을 보다 유연하고 동적으로 적용할 수 있는 능동적인 보안 기능을 제공할 수 있어야 하며, 네트워크 보안 환경 변화에 보다 민감하고 신속하게 대응할 수 있는 지능적인 보안 기능을 제공할 필요가 있다.

먼저, 능동보안 기술에 대해 설명하기로 한다. 능동보안 기술에서의 요구조건을 만족시키기 위해 필요한 요소기술은 다음과 같다. 첫째로는, 제한적인 특정 내부망의 보안 관리에서 인터넷과 같은 광역 네트워크에서 동작하는 보안 관리 기능이다. 둘째로는, 보안관리영역(도메인) 간의 상호 결합적 협업 기능이다. 셋째로는, 새로운 공격에 대한 탐지 및 대응 메커니즘을 시스템의 변경 없이 동적으로 수용할 수 있으며, 실행이 가능한 유연한 보안 기반 구조이다. 네째로는, 네트워크 공격을 감행한 침입자를 파악하고 감시하며, 보안정책에 의해 네트워크로부터 고립화시키는 능동적인 대응 기술이다. 다섯째로는, 네트워크의 보안 상태를 적극적으로 감시하고, 보안환경 변화에 민감하게 반응하는 기능이다. 상기의 요구 조건을 만족하는 보안 메커니즘 및 프레임워크를 실현하기 위한 기술을 능동 보안 기술이라 말한다. 도 1은 능동보안 관리 프레임워크 및 메카니즘을 도시한 것이다.

다음으로 능동보안관리 프레임워크를 설명하기로 한다. 액티브 네트워크를 이용한 능동보안관리 프레임워크는 도 1에 도시한 바와 같이 가입자 네트워크 상에 액티브 네트워킹 기능을 제공하는 능동보안노드(100)와 이들을 제어하는 능동보안관리시스템(110)으로 구성되며, 논리적인 하나의 보안관리 도메인을 형성한다. 또한 각 보안 관리 도메인은 전체 네트워크 상에 분산적으로 배치되며 상호간의 연동 및 협업을 위한 별도의 관리 계층은 갖지 않는다. 즉, 모든 능동 보안 제어는 액티브 패킷을 통해 이루어지며 보안 도메인 간의 상호 연동과 협업 역시 액티브 패킷에 의해 수행된다.

도 2는 능동보안 시스템 플랫폼(Platform) 구조를 도시한 것이다. 능동보안노드에는 도 2와 같이 이동 보안 센서를 수신하고 실행시킬 수 있는 능동센서(active sensor) 처리엔진이 탑재되며, 능동보안관리시스템에는 능동보안관리를 위한 응용프로그램(application)이 추가적으로 탑재된다. 능동보안관리 프레임워크의 각 구성요소에 대해 기술하고, 각각에 대한 주요 기능을 설명하면 다음과 같다.

먼저, 액티브 네트워킹(active networking)을 설명하기로 한다. 컴퓨터의 고성능화, 인터넷의 보급 및 WWW(World Wide Web)등의 새로운 네트워크 어플리케이션의 등장에 의해 네트워크 컴퓨팅이 비약적으로 발전하는 것에 반해 네트워크 상에서 노드 간의 통신 기반이 되는 네트워크 프로토콜의 발전은 매우 늦은 편이다. 이는 네트워크 간의 상호 운용성을 확보하기 위한 프로토콜 표준화가 새로운 기술 개발에 비해 매우 늦은 속도로 진행되기 때문이다. IETF, ISO 등 표준화 단체에 의한 표준화 작업에는 많은 노력과 시간이 소요되며 프로토콜이 규정되어도 실제 네트워크 상에 적용되어 운용되기까지는 더욱 많은 기간이 필요하다. 이러한 인터넷 상에서의 문제를 해결하기 위하여 DARPA(Defense Advanced Research Project Agency)에서는 유연하고 고기능을 제공하는 네트워크를 실현하기 위한 기술로 액티브 네트워크 개념을 제안했다.

액티브 네트워크란 패킷 스위칭 네트워크를 통해 전송되는 이동 프로그램을 실행할 수 있는 라우터나 스위치를 배치하여, 전송된 액티브 패킷에 포함되어 있는 이동 프로그램을 서비스 특성이나 사용자 요구에 따라 적합하게 연산, 처리할 수 있는 네트워크이다. 즉, 사용자에게 네트워크를 프로그래밍하는 능력을 부여하는 네트워크 아키텍처를 액티브 네트워크라고 한다. 능동보안관리 프레임워크의 네트워크 인프라(Infra)는 액티브 네트워크로 구성된다. 액티브 네트워크를 이용할 경우 네트워크 보안이 능동적으로 발전할 수 있는 이유는 크게 다음과 같다. 첫째, 네트워크 상의 라우터(Router)나 스위치들은 자신에게 전송된 보안 대응 프로그램을 특별한 프로토콜이 없이도 네트워크 처리 단계에서 인식하고 수행할 수 있다. 둘째, 보안 관리자는 각각의 노드에서 필요한 보안대응 부를 프로그래밍에 의해 제어 할 수 있다. 즉 네트워크 상에서의 보안 메커니즘을 보다 유동적이고 유연하게 배치하고 삭제할 수 있으며 다수의 네트워크 장비 및 보안장비를 분산 관리할 수 있다.

이는 제품 개발시 탑재된 보안 기능을 정해진 프로토콜에 의해 상호 연동시키며, 제한된 범위에서의 보안 기능만을 제공할 수 있었던 기존의 정적인 보안 메커니즘의 문제들을 해결할 수 있는 새로운 개념의 보안 메커니즘이다. 광역 네트워크 상에 분산적으로 설치되어있는 다수의 보안 노드에 대한 보안 제어 기능과 노드간의 협업 기능을 제공하는 능동적인 네트워크 보안 프레임워크를 제공하기 위해서는 보안 기능의 복잡한 계층 구조화와 이들간의 통신을 위한 다수의 프로토콜이 제공되어야 한다. 액티브 네트워크를 이용한

네트워크 보안 프레임워크에서는 프로토콜 대신 액티브 패킷을 이용하며, 보안 기능 자체를 액티브 패킷 내의 보안 대응 프로그램으로 전송하고 실행함으로써 보안 구조를 단순화시키고 네트워크 자원을 절약한다.

능동보안관리 실행 환경에 대해 설명한다. 액티브 네트워크에서 이동 보안 센서를 이용하여 네트워크의 보안상태를 관리하기 위해서는 보안관리 도메인 내의 각 보안 시스템에 네트워크 계층에서 이동 보안 센서를 인지하고 실행시킬 수 있는 기능이 탑재되어 있어야 한다. 또한 능동보안관리시스템에는 보안관리 기능을 수행하기 위한 능동보안관리 엔진이 탑재되어야 한다. 이처럼 능동보안관리 실행 환경은 이동 보안 센서 처리 블록과 능동보안관리 블록으로 구성된다.

이동보안센서 처리엔진을 설명하기로 한다. 도 3은 이동보안센서 처리 엔진 및 능동보안관리 엔진의 기능 블록을 도시한 것이며 각 블록의 기능은 다음과 같다. 능동패킷처리부(Active Packet Processing, 300)는 액티브 패킷 형태로 전송되는 이동 보안 센서를 네트워크 계층에서 인식하고 수신하여 이동 보안 센서 실행부로 전달하는 기능 및 새로이 생성된 이동 보안 센서를 능동 패킷으로 캡슐화하여 네트워크에 전송하는 기능을 수행한다.

보안대응센서 실행부(Security Sensor Execution Enviornment, 320)는 능동패킷 처리부로부터 이동 보안 센서를 수신하여 제한된 컴퓨팅 자원 내에서 실행시키는 기능을 수행한다. 이때 실행되는 코드가 센서 내에 포함되어 있지 않은 경우에는 코드 서버에서 다운로드 받아 실행한다. 이동 보안 센서의 수행에 필요한 자원 할당과 새로이 생성된 이동 보안 센서를 네트워크에 전송 하는 기능은 하위 계층의 능동패킷 처리부에 요구한다. 이동보안센서(Mobile Security Sensor, 340)는 액티브 네트워크 내의 보안 노드에서 실제 수행되어야 하는 보안대응 정책 정보 또는 실행 프로그램이 저장되어 있는 실행 가능한 이동성 어플리케이션을 제공한다.

보안대응수행 인터페이스부(Security Enforcement Interface, 310)는 이동 보안 센서가 여러 이기종 노드의 보안 대응 기능을 일원적으로 제어하기 위한 추상화된 인터페이스를 제공하는 기능을 수행한다. 즉, 이동 보안 센서가 패킷 필터링 또는 블록킹과 같은 네트워크 노드에서 실질적으로 실행되는 보안 대응 기능을 제어하기 위한 통일적인 인터페이스들을 제공한다. 보안 대응 수행 인터페이스부는 각 네트워크 노드에서 제공되는 보안 대응 기능의 차이를 흡수하고, 공통된 본질적인 기능만을 추상화함으로써 통일된 이동 보안 센서 개발 방법을 제공한다.

능동보안관리엔진(330)은 능동보안관리시스템(Active Security Management System)에 탑재되는 어플리케이션 엔진이며, 보안 도메인 내의 각 보안 시스템으로부터 보고된 보안 위배 행위에 대해 능동 보안 대응을 수행함으로써 네트워크의 보안 상태를 자동적으로 제어하는 기능을 제공하는 소프트웨어 엔진이다.

능동보안관리 기능은 이동 보안 센서를 생성하여 네트워크에 송신하거나 수신된 이동 보안 센서를 실행함으로써 발생하는 보안 대응 행위에 대한 모든 정보를 관리한다. 또한 네트워크에 전송한 보안 대응 센서로부터 수집되는 네트워크 보안 상태 정보를 관리하고 이에 대한 보안 대응 부(이동 보안 센서)을 네트워크에 제공함으로써 네트워크 차원의 보안 상태를 동적으로 제어하고 관리한다. 도 4는 능동보안관리 센서의 기능구조를 도시한 것이며 각 기능은 다음과 같다.

보안 위배 이벤트 정합부(Security Alert I/F, 400)는 보안 관리 도메인에 설치되어 있는 침입탐지 시스템 또는 방화벽과 같은 보안 시스템으로부터 송신되는 경보 데이터를 실시간으로 수집하는 기능을 수행한다. COPS, IAP, SNMP 등 개발사 별로 다양한 프로토콜을 통해 전송되는 경보 데이터를 수집하기 위해 각 프로토콜을 정합하기 위한 다중 프로토콜 정합 기능을 제공한다.

보안 정책 결정부(Security Policy Decision, 410)는 탐지된 보안 위반 행위에 대해 어떠한 대응 부를 실행할 것인가를 판단하는 기능을 수행한다. 보안대응실행부(Security Response, 420)는 침입자 역 추적, 침입자 고립화, 패킷 블록킹 등과 같은 실질적인 대응을 실행하기 위한 센서를 생성하여 결정된 보안정책을 네트워크에 배포하는 기능을 수행한다. 센서 관리부(Sensor Manager, 430)는 네트워크에 송수신되는 모든 센서의 정보 및 수행 상태를 데이터베이스시스템에 저장하고 관리하는 기능을 수행한다. 센서 정보를 관리함으로써 타 도메인에 요청한 보안 대응 상태를 파악할 수 있다. 이벤트 관리부(Event Manager, 440)는 이동 보안 센서 처리 엔진과 송수신 센서에 대한 정보를 교환하기 위한 메시지 처리 및 관리 기능을 수행한다. 즉, 보안정책결정에 의해 전송하여야 하는 센서에 재한 정보 및 타 도메인으로부터 수신된 센서에 대한 정보를 이동 보안 센서 처리 엔진과 교환하기 위한 기능 모듈이다. 관리자정합부(Security Manager GUI I/F, 450)는 보안관리자에게 보안 관리 상태를 보고하고, 관리자의 수동적인 개입을 수용하여 보안 메커니즘에 적용시키는 기능을 수행한다.

능동보안관리 시나리오에 관해 설명하기로 한다. 액티브 네트워크를 이용한 능동보안 프레임워크 상에서 동작하는 능동 보안 기능의 한 예인 위조된 IP 역추적(Spoofed IP Trace back)에 대해 기술한다. Spoofed IP 공격은 대다수의 DDoS 공격에서 이용되는 수법으로 패킷 내의 근원지 IP 주소를 위조하여 침입 근원지를 속이는 공격 방법이다. 제안하는 시나리오에서는 이러한 한 공격에 실제 패킷의 송신자를 추적하여 네트워크로부터 고립화 시키기기 위한 역추적 메카니즘이다.

이를 실현하기 위해 각 보안영역(Secure Domain)의 망 접속 점(Edge Point)에 설치된 능동보안노드(MoSE : Mobile Security Engine)에서는 Ingress Filtering 기능을 수행하여 해커에 의한 타 도메인의 IP 주소 위조 및 조작을 사전에 방지하도록 하여 IP Spoofing 가능 범위를 하나의 보안 도메인 내부로 한정시킨다. 도 5는 액티브 네트워크를 이용한 능동보안관리 프레임워크에서의 Spoofed IP 역 추적 메커니즘 및 기능절차를 도시한 것이다.

상기 시나리오에 대한 일련의 절차는 다음과 같다. 제1단계는 IP 주소 위장단계로서, 보안영역(Secure Domain) A에 위치한 해커(Hacker) A는 같은 도메인에 위치하는 호스트A의 IP주소를 자신의 IP 주소로 위조한다. 제2단계는 타 도메인에 있는 서버 공격단계로서, 보안영역(Secure Domain) B에 위치하는 서버 B에게 flood 계열의 DoS(Denial of Service) 공격을 시도한다. 제3단계는 침입탐지 경보 전달로서, 보안영역 B에 존재하는 SGS_IDS는 공격을 감지하여 침입탐지 경보를 능동보안관리시스템 B(ASMS-B)로 송신하며, 여기서 침입탐지 경보에는 탐지된 유해 패킷에 대한 축약정보 및 탐지 정보가 포함되어 있다. 제4단계는 패

킷 차단(block) 센서 전송단계로서, 능동보안관리시스템 B(ASMS-B)는 수신된 침입탐지 경보로부터 유해 패킷의 송신 근원지 IP주소(위조당한 호스트A의 IP 주소)를 검출하고, 해당 IP 주소로부터의 유해 패킷 유입을 차단하기 위해 패킷 차단 센서를 생성한 후 자신의 도메인 접속 점에 위치하는 MoSE-B로 패킷 차단 센서를 전송한다. 제5단계는 패킷 차단 센서 실행단계로서, 패킷 차단 센서를 수신한 MoSE-B는 수행환경을 통해 수신된 블록킹 센서를 실행하여 유해 패킷의 유입을 차단하도록 한다. 따라서 MoSE-B는 해커의 위조 패킷은 물론 IP 주소를 위조 당한 호스트A의 정상적인 패킷까지 차단된다. 제6단계는 역추적 센서 전송단계로서, 능동보안관리시스템 B(ASMS-B)는 (단계 3)에 의해 수신된 침입탐지 경보 데이터를 참조하여 유해 패킷을 송신한 근원지 IP 주소를(보안영역 A의 호스트A 근원지 IP주소) 목적지 주소로 하여 역추적 센서를 생성하여 전송한다. 제7단계는 역추적 센서 실행단계로서 상기 제6단계에서 송신한 역추적 센서는 보안영역 A의 접속 점에 위치하는 MoSE-A에서 수신되어 실행된다. 역추적 센서는 로깅 센서에 의해 기록된 Outgoing 이더넷 프레임 축약 정보를 검색하여 유해 패킷 정보와 일치하는 로그 정보를 추출한 후, 로그 정보에 기록된 Mac 근원지 주소와 ARP 테이블에 저장된 IP 주소를 비교하여 위조 여부 및 실제 근원지 IP 주소를 파악한다. 제8단계는 역추적 센서 실행 결과 보고 단계로서, 역추적 의뢰 정보, 성공 여부,파악된 근원지 주소 등의 정보를 해당 도메인에 위치하는 ASMS-A로 송신한다. 제9단계는 침입자 고립을 위한 패킷 차단 센서 전송 단계로서, 역추적 센서 실행 결과를 수신한 ASMS-A는 파악된 근원지 주소로부터의 패킷 송신을 원천 봉쇄하기 위해서 탐지된 부정 사용자의 MAC 근원지 주소로부터의 패킷 포워딩을 차단하는 패킷 블록킹 센서를 MoSE-A에게 전송한다. 제10단계는 침입자 원천봉쇄 결과 보고 단계로서, 능동보안관리시스템 A(ASMS-A)는 역추적을 의뢰한 능동보안관리시스템 B(ASMS-B)로 최종 역추적 결과 및 대응 정보를 전송한다. 제11단계는 정상적인 패킷에 대한 세션 복구를 위한 차단 해제 센서를 전송하는 단계로서, ASMS-B는 단계 5에서 IP 주소를 위조 당한 호스트A의 정상적인 패킷까지 차단한 세션을 복구하기 위해 차단 해제 센서를 생성하여, MoSE-B로 차단 해제 센서를 전송한다. 제12단계는 정상적인 패킷에 대한 세션 복구를 위한 차단 해제 센서 실행하는 단계로서, 차단 해제 센서를 수신한 MoSE-B는 단계 5에서 IP 주소를 위조를 당한 호스트A의 정상적인 패킷을 차단한 세션을 복구한 후, 복구된 결과를 ASMS-B로 통보한다. 따라서 MoSE-B는 해커의 위조 패킷 및 해커의 근원지 IP 주소로부터의 패킷 유입은 검출되지 않고 위조 당한 호스트 IP 주소로부터의 정당한 패킷 유입은 허락된다. 제13단계는 보안관리자에 통보하는 단계로서, ASMS-B는 제10단계 및 제12단계에서 수신된 역추적 보고센서의 정보를 보안관리자에게 통보한다.

한편, 본 발명에 따른 유해트래픽 탐지 및 대응 시스템 및 그 방법을 상세히 설명하기로 한다. 도 6은 본 발명에 따른 유해 트래픽 탐지 및 대응 시스템이 기능하기 위한 액티브 네트워크를 이용한 네트워크 보안 프레임워크와 망 구성을 도시한 것이다. 상기 액티브 네트워크를 이용한 네트워크 보안 프레임워크 및 망은 적어도 둘 이상의 보안관리 영역을 포함하며 분산되어 있다. 도 6에서는 상기 보안관리 영역은 3개 도시되어 있으며, 광역 망의 접속점에 위치하여 보안기능을 수행하는 능동보안노드시스템(600, 620, 630) 및 보안관리 영역에서 발생한 보안위배 행위에 대해 대응하고 보안상태를 제어하는 능동보안관리 시스템(610, 640, 650)을 포함한다.

도 7은 본 발명에 따른 유해 트래픽 탐지 및 대응 시스템을 블록도로 도시한 것으로서, 트래픽 모니터링부(700), 유해 트래픽 추적관리부(710), 유해트래픽 추적부(720) 및 유해트래픽 차단보고부(730)로 이루어진다.

상기 트래픽 모니터링부(700)는 네트워크의 접속점에 위치하는 능동보안노드 시스템(600, 620, 630)에서 실행되며, 광역 망의 접속 점에 위치하는 능동보안노드 시스템(600, 620, 630)으로 유입되는 트래픽의 변동을 주기적으로 감시하고, 사전에 설정한 기준치를 초과하는 트래픽 변동이 감지되면 이에 대한 이벤트 정보를 트래픽 감사 센서를 통해 능동보안관리 시스템(610, 640, 650)으로 송신한다. 상기 기준치는 월별, 일별, 시간대 별로 구성된 트래픽 임계수치(threshold)가 될 수 있으며, 상기 임계수치와 비교 분석한다.

상기 유해트래픽 추적관리부(710)는 능동보안관리시스템(610, 640, 650)에서 실행되며, 상기 능동보안관리시스템으로 전달된 트래픽 감사 센서의 이벤트 정보로부터 유해 트래픽 추적 여부를 결정하고, 유해트래픽 추적부(720)를 생성하여 관리 도메인에 위치하는 능동보안노드시스템(600)으로 전송한다.

상기 유해트래픽 추적부(720)는 고정형 및 이동형으로 구현될 수 있으며, 이동형일 경우 능동보안관리시스템(610, 640, 650) 및 능동보안노드 시스템(600, 620, 630) 간에 이동한다. 상기 유해트래픽 추적부(720)는 사전에 설정한 기준치를 초과하는 트래픽 성분을 갖는 IP 주소(근원지 IP 주소와 목적지 IP 주소의 쌍)를 검출하고, 근원지 IP 주소가 위치하는 네트워크에 위치하는 능동보안노드 시스템(620)으로 이주하며, 해당 근원지 IP 주소에서 송신되는 트래픽을 세션별로 분석한 후 사전에 설정한 기준치를 초과하는 세션 트래픽을 검출하여 차단하고 유해 트래픽 탐지 및 대응 결과를 해당 보안 관리 영역 내의 능동보안관리 시스템(640)으로 전달한다.

상기 유해트래픽 차단보고부(730)는 유해트래픽 탐지 및 대응 결과를 최초에 유해트래픽 추적을 요구한 능동보안관리 시스템(610)에게 통보한다.

다음으로 도 8은 본 발명에 따른 유해트래픽 탐지 및 대응 시스템의 동작을 설명하기 위한 절차를 도시한 것으로서, 도 8을 참조하여 그 동작을 설명하기로 한다. 도 8에 도시한 바와 같이 네트워크의 접속점에 위치하는 능동보안노드 시스템(800)에서 실행되고 있는 트래픽 모니터링부(700)는 능동보안노드 시스템(800)으로 유입되는 트래픽의 변동을 주기적으로 감시하고, 월별, 일별, 시간대 별로 구성된 트래픽 임계수치(threshold)와 비교 분석한 결과 기준치를 초과하는 트래픽 변동이 감지되면 이에 대한 이벤트 정보를 트래픽 감사 센서를 통해 능동보안관리 시스템으로 송신한다.(1단계) 능동보안관리 시스템에서 실행되고 있는 유해트래픽 추적관리부(710)는 전달된 트래픽 감사 센서의 이벤트 정보로부터 근원지 주소와 네트워크 침입탐지 경보 및 블랙리스트 조회 등을 통해 유해 트래픽 추적 여부를 결정하고, 유해 트래픽 추적부(720)를 생성하여 트래픽 감사 센서를 전달한 능동보안노드 시스템(800)으로 송신한다.(2단계)

능동보안노드 시스템(800)으로 전달된 유해트래픽 추적부(710)는 능동보안노드 시스템(800)으로 유입되는 트래픽을 IP 주소 단위(근원지 IP 주소와 목적지 IP 주소의 쌍)로 분석하고, 보안관리자에 의해 설정된 IP 트래픽 임계수치를 초과하는 유해 IP 주소들을 검출한다. 또한 검출된 유해 IP 주소들을 참조하여 해당 유해 IP 주소의 네트워크에 위치하는 각 능동보안노드 시스템(820)으로 자신을 복제하여 이동한다. 상기 기

능 절차에 의해 각 능동보안노드 시스템으로 전달되어 수행되는 유해 트래픽 추적부(710)는 해당 유해 IP 주소로부터의 트래픽을 세션 단위로 분석한 후 보안관리자가 설정한 기준치를 초과하는 세션 트래픽을 검출하여 해당 세션 트래픽을 차단한다. 또한 유해 트래픽 탐지 및 대응 결과를 능동보안관리 시스템으로 통보하기 위해 능동보안관리 시스템(830)으로 이동한다.(3단계) 능동보안관리 시스템에서 실행되고 있는 유해트래픽 추적관리부(710)가 상기 유해트래픽 추적부(720)를 통해 유해 트래픽 탐지 및 대응 결과를 수신하면 센서의 정보를 참조하여 최초에 유해 트래픽 추적을 요구한 능동보안관리 시스템(810)으로 유해 트래픽 차단 보고부(730)를 생성하여 전달한다.(4단계)

한편, 상기 트래픽 모니터링부(700), 유해 트래픽 추적관리부(710), 유해트래픽 추적부(720) 및 유해트래픽 차단보고부(730)는 소프트웨어적으로 구현하고자 할 수 있으며, 예를 들어 객체지향 프로그래밍 언어인 자바(Java)로 구현할 때에는 트래픽 모니터링 센서(700), 유해 트래픽 추적관리 센서(710), 유해트래픽 추적 센서(720) 및 유해트래픽 차단보고 센서(730)로 명명하기도 한다.

상술한 바와 같이 본 발명은 컴퓨터로 읽을 수 있는 기록매체에 컴퓨터가 읽을 수 있는 코드로서 구현하는 것이 가능하다. 컴퓨터가 읽을 수 있는 기록매체는 컴퓨터 시스템에 의하여 읽혀질 수 있는 데이터가 저장되는 모든 종류의 기록시스템을 포함한다. 컴퓨터가 읽을 수 있는 기록매체의 예로는 ROM, RAM, CD-ROM, 자기 테이프, 플로피디스크, 광 데이터 저장시스템 등이 있으며, 또한 캐리어 웨이브(예를 들어 인터넷을 통한 전송)의 형태로 구현되는 것도 포함한다. 또한 컴퓨터가 읽을 수 있는 기록매체는 네트워크로 연결된 컴퓨터 시스템에 분산되어, 분산방식으로 컴퓨터가 읽을 수 있는 코드가 저장되고 실행될 수 있다.

발명의 효과

따라서 상술한 본 발명에 따르면, 네트워크 자원 및 서비스를 고갈시키는 대역폭 소모형 분산 서비스 거부 공격과 같은 유해 트래픽을 조기에 탐지하고, 유해 트래픽 근원지를 추적하여 원천봉쇄하는 기능을 제공함으로써 시스템 보호 및 네트워크 자원 보호의 기능을 제공할 수 있다.

(57) 청구의 범위

청구항 1

분산된 적어도 둘 이상의 보안관리 영역을 포함하는 능동 네트워크 보안 프레임 워크에 있어서,

상기 보안관리 영역은 광역 망의 접속점에 위치하여 보안기능을 수행하는 보안노드 시스템 및 보안관리 영역에서 발생한 보안위배 행위에 대해 대응하고 보안상태를 제어하는 보안관리 시스템을 포함할 때,

상기 보안노드 시스템으로 유입되는 트래픽의 변동을 감시하고, 소정의 기준치를 초과하는 트래픽 변동이 감지되면 이에 대한 이벤트 정보를 당해 보안관리 영역의 보안관리 시스템으로 송신하는 트래픽 모니터링부;

상기 보안관리 시스템으로 전달된 이벤트 정보로부터 유해 트래픽 추적 여부를 결정하고, 이를 당해 보안노드 시스템으로 전송하는 유해트래픽 추적관리부; 및

소정의 기준치를 초과하는 트래픽 성분을 갖는 근원지 IP 주소와 목적지 IP 주소를 검출하고, 근원지 IP 주소가 위치하는 보안관리 영역에 위치하는 보안노드 시스템 상에서, 상기 근원지 IP 주소에서 송신되는 트래픽을 분석한 후 소정의 기준치를 초과하는 트래픽을 검출하여 차단하고 유해 트래픽 탐지 및 대응 결과를 해당 보안 관리 영역 내의 보안관리 시스템으로 전달하는 유해트래픽 추적부를 포함함을 특징으로 하는 네트워크에서의 유해패킷 탐지 및 대응 시스템.

청구항 2

제1항에 있어서,

유해 트래픽 탐지 및 대응 결과를 최초에 유해 트래픽 추적을 요구한 능동보안관리 시스템에게 통보하는 유해트래픽 차단보고부를 더 구비함을 특징으로 하는 네트워크에서의 유해트래픽 탐지 대응 시스템.

청구항 3

네트워크의 트래픽의 변동을 감시하여 소정이 기준치를 초과하는 트래픽 변동이 감지되면 이에 대한 이벤트정보를 송신하는 제1단계;

상기 이벤트정보를 수신하여 유해 트래픽 추적 여부를 결정하는 제2단계; 및

추적이 필요하다고 판단되면, 상기 소정의 기준치를 초과하는 트래픽의 근원지 주소를 검출하고, 상기 근원지 주소에서 송신되는 트래픽을 분석한 후 소정의 기준치를 초과하는 트래픽을 차단하는 제3단계를 포함함을 특징으로 하는 네트워크에서의 유해패킷 탐지 및 대응 방법.

청구항 4

제3항에 있어서, 상기 제2단계는

소정의 기준치를 초과하는 트래픽의 근원지 IP 주소 및 목적지 IP 주소를 검출하고, 상기 근원지 IP주소가 위치하는 네트워크 상의 소정의 시스템에서 상기 근원지 IP 주소로부터 송신되는 트래픽을 분석한 후 소정의 기준치를 초과하는 트래픽을 차단하는 단계임을 특징으로 하는 네트워크에서의 유해패킷 탐지 및 대응 방법.

청구항 5

제3항 또는 제4항에 있어서,

상기 제3단계의 유해 트래픽 탐지 및 대응 결과를 유해 트래픽 추적을 요구한 시스템에 통보하는 단계를 더 구비함을 특징으로 하는 네트워크에서의 유해패킷 탐지 및 대응 방법.

청구항 6

분산된 적어도 둘 이상의 보안관리 영역을 포함하는 능동 네트워크 보안 프레임 워크에 있어서,

상기 보안관리 영역은 광역망의 접속점에 위치하여 보안기능을 수행하는 보안노드 시스템 및 보안관리 영역에서 발생한 보안위배 행위에 대해 대응하고 보안상태를 제어하는 보안관리 시스템을 포함할 때,

상기 보안노드 시스템으로 유입되는 트래픽의 변동을 감시하고, 소정의 기준치를 초과하는 트래픽 변동이 감지되면 이에 대한 이벤트 정보를 상기 보안관리 시스템으로 송신하는 제1단계;

보안관리 시스템으로 전달된 이벤트 정보로부터 유해 트래픽 추적 여부를 결정하고, 유해 트래픽 추적 센서를 생성하여 관리 도메인에 위치하는 보안노드 시스템으로 전송하는 제2단계; 및

소정의 기준치를 초과하는 트래픽 성분을 갖는 근원지 IP 주소와 목적지 IP 주소를 검출하고, 근원지 IP 주소가 위치하는 로컬 네트워크 상의 보안노드 시스템들에게 자신을 복제하여 전송하며, 해당 능동보안노드 시스템으로 이주한 후에는 해당 근원지 IP 주소에서 송신되는 트래픽을 서비스 포트 별로 분석한 후 소정의 기준치를 초과하는 트래픽을 검출하여 차단하는 제3단계를 포함함을 특징으로 하는 네트워크에서의 유해트래픽 탐지 및 대응 방법.

청구항 7

제6항에 있어서, 상기 제2단계는

보안관리 시스템으로 전달된 이벤트 정보로부터 유해 트래픽 추적 여부를 결정하고, 유해 트래픽 추적 센서를 생성하여 관리 도메인에 위치하는 보안노드 시스템으로 전송하고 유해 트래픽 탐지 및 대응 결과를 해당 보안 관리 영역 내의 보안관리시스템으로 전달하는 단계이고,

유해 트래픽 탐지 및 대응 결과를 최초에 유해 트래픽 추적을 요구한 보안관리 시스템에게 전달하는 단계를 더 구비함을 특징으로 하는 네트워크에서의 유해트래픽 탐지 및 대응 방법.

청구항 8

제6항 또는 제7항에 있어서, 상기 이벤트 정보는

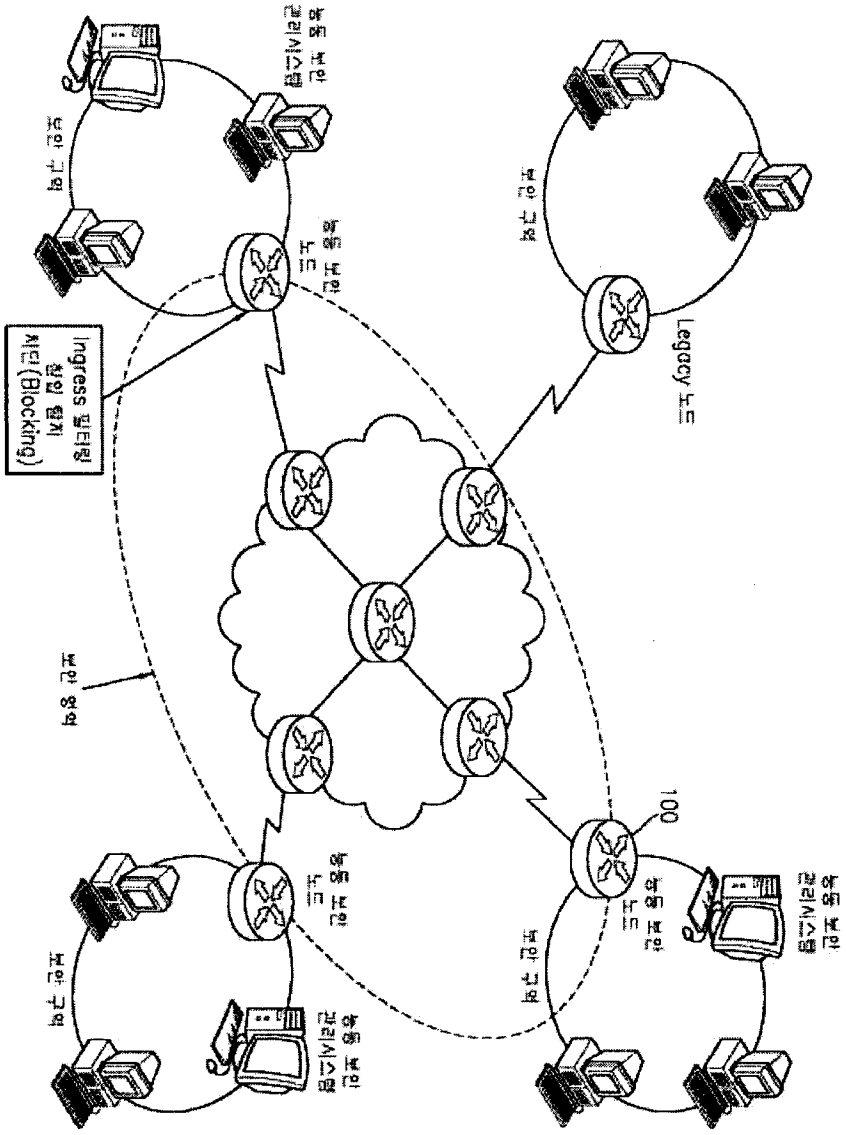
트래픽 감사 센서를 통해 보안관리 시스템으로 송신함을 특징으로 하는 네트워크에서의 유해트래픽 탐지 및 대응 방법.

청구항 9

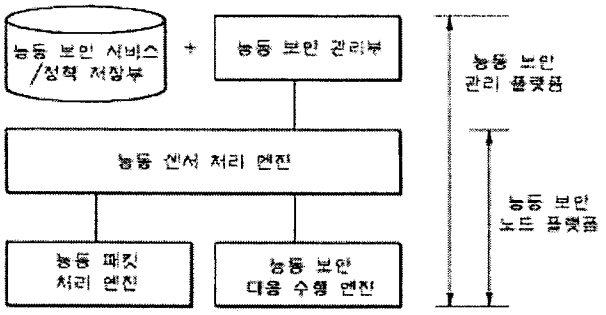
제3항 내지 제8항 중 어느 한 항에 기재된 발명을 컴퓨터에서 실행시키기 위한 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록매체.

도면

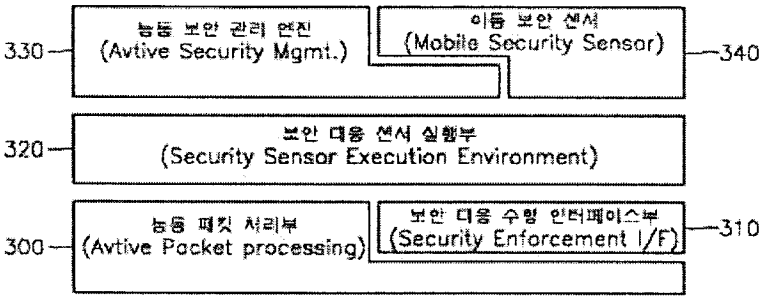
도면1



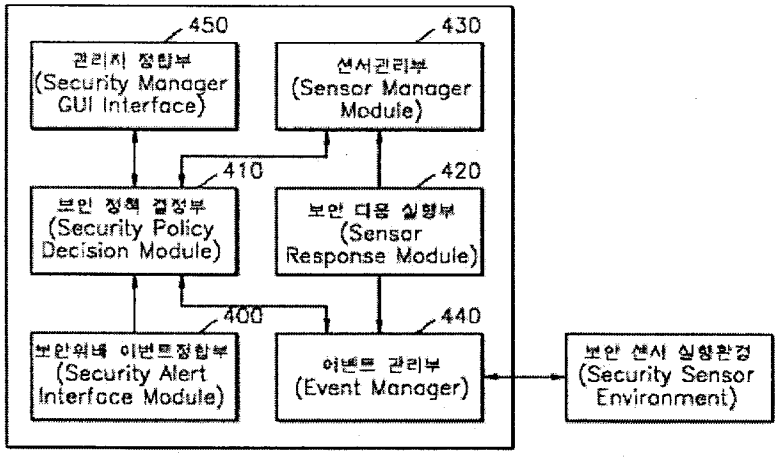
도면2


능동 보안 서비스
/정책 저장부
+
능동 보안 관리부
능동 보안
관리 플랫폼
능동 센서 처리 엔진
능동 보안
노드 플랫폼
능동 패킷
처리 엔진
능동 보안
대응 수행 엔진

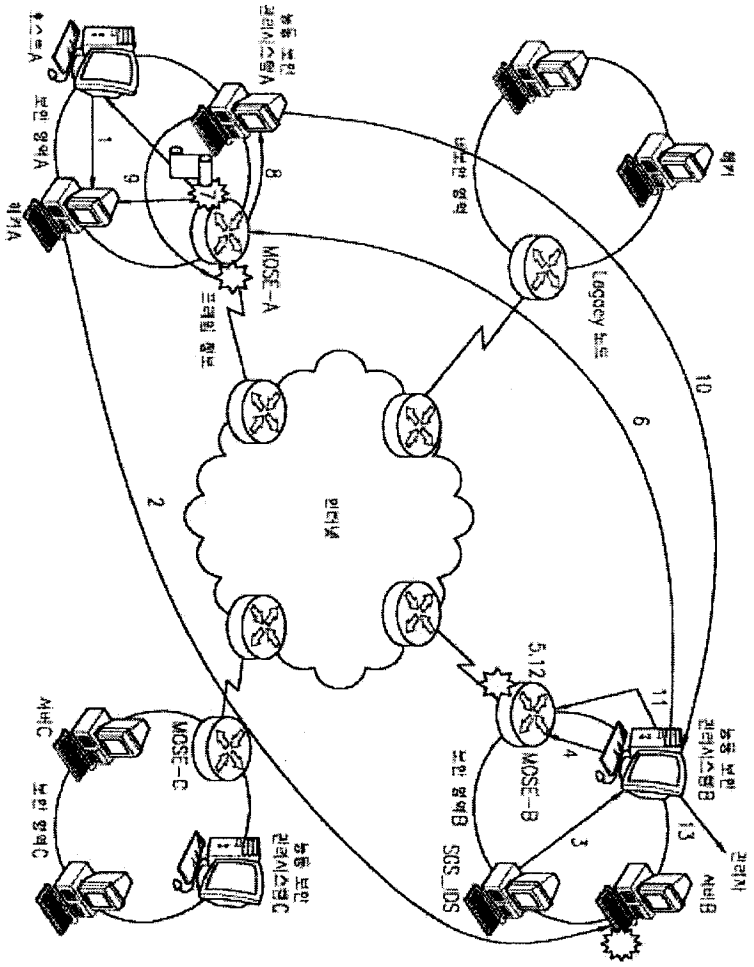
도면3


330
능동 보안 관리 엔진
(Avtive Security Mgmt.)
이동 보안 센서
(Mobile Security Sensor)
340
320
보안 대응 센서 실행부
(Security Sensor Execution Environment)
300
능동 패킷 처리부
(Avtive Packet processing)
보안 대응 수행 인터페이스부
(Security Enforcement I/F)
310

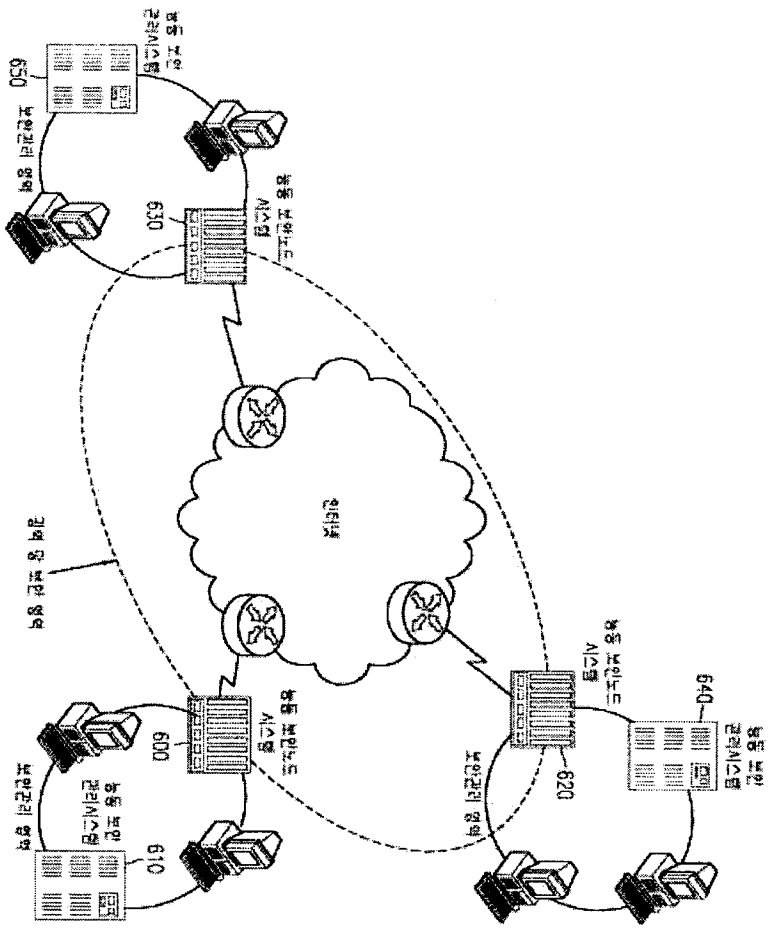
도면4


450
관리자 정합부
(Security Manager
GUI Interface)
430
센서관리부
(Sensor Manager
Module)
410
420
보안 정책 결정부
(Security Policy
Decision Module)
보안 대응 실행부
(Sensor
Response Module)
400
440
보안위협 이벤트정합부
(Security Alert
Interface Module)
이벤트 관리부
(Event Manager)
보안 센서 실행환경
(Security Sensor
Environment)

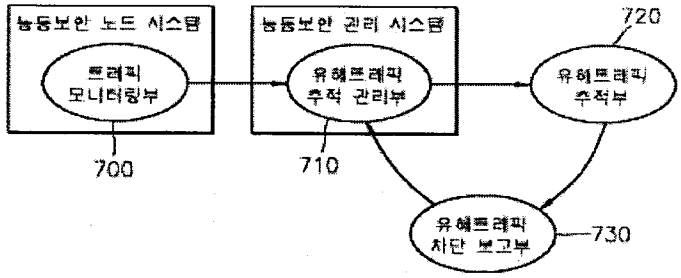
도면5



도면6



도면7


능동보안 노드 시스템
트래픽 모니터링부
700
능동보안 관리 시스템
유해트래픽 추적 관리부
710
720
유해트래픽 추적부
유해트래픽 차단 보고부
730

도면8